EXHIBIT 8

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with Six Email Accounts Maintained at Premises Controlled by Google, LLC, USAO Reference No. 2022R00863

24 MAG 56

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

Marco Dias, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Special Agent with Internal Revenue Service-Criminal Investigation ("IRS-CI") for approximately four years. I am currently assigned to the Cyber and Cryptocurrency Investigation Unit, which focuses on investigating crimes involving, among other things, financial fraud schemes and money laundering using cryptocurrency. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. During the course of my duties, I have received training about and participated in the execution of search warrants, and the review and analysis of both physical and electronic evidence.

B. The Provider, the Subject Account and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the email accounts listed below (collectively, the "Subject Accounts"), maintained by Google, LLC ("Google" or the "Provider"):

Account Identifier	**Account User**[1]	**Referred to Herein**
anton-pine-needle@18decimal.io	Anton Peraire-Bueno	Subject Account-1
james-pine-needle@18decimal.io	James Peraire-Bueno	Subject Account-2
anton@18decimal.io	Anton Peraire-Bueno	Subject Account-3
james@18decimal.io	James Peraire-Bueno	Subject Account-4
antonperairebueno2000@gmail.com	Anton PB	Subject Account-5
jamesperairebueno@gmail.com	James Peraire	Subject Account-6

The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of a cryptocurrency fraud scheme, involving a computer exploit, in or about April 2023 in violation of 18 U.S.C. §§ 1343 and 1349 (wire fraud and conspiracy to commit wire fraud); 18 U.S.C. § 1030 (computer fraud); 18 U.S.C. § 371, 7 U.S.C. § 9(1) and 13(a)(5), and 17 C.F.R. § 180.1 (commodities fraud and conspiracy to commit commodities fraud); 7 U.S.C. § 13(a)(2) (commodities fraud manipulation); and 18 U.S.C. §§ 1956 and 1957 (money laundering and conspiracy to commit money laundering) (collectively, the "Subject Offenses") in connection with a computer exploit executed in or about April 2023. This

[1] Information about the account user is based on my review of records provided by Google in response to grand jury subpoenas.

affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

4. I have learned the following about the Provider:

a. Google is a United States company that offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the free email domain name gmail.com . A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents*. Google allows subscribers to maintain email accounts under the domain name "gmail.com" or an independently selected domain name followed popular domain extensions like .io, .com, and/or .org. Google also allows subscribers to maintain email aliases that are alternate email addresses associated with a single Google address. For example, if an individual's primary email address is "johndoe@gmail.com," Google allows the individual to create an email alias such as "jdoe@gmail.com" and all messages sent to the alias address are delivered to the primary email address. Like other online email providers, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the

subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Contacts.* Google also allows subscribers to maintain the equivalent of an address book, called "Contacts," comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Web & App Activity, Search, Chrome, and Browsing History.* Google maintains a history of a subscriber's websites visited, devices used, applications (or "apps") used, Google search query history, Chrome usage, and browsing records. For some accounts, Google maintains "My Activity" records for a subscriber, which include records of web searches, image searches, video searches, news browsing, map activity, and analytics on the account.

vi. *Google Drive Content*. Google also provides account holders access to "Google Drive" which enables users to back up documents, images, chat history, emails, and other files. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

vii. *Google Docs and Google Sheets*. Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive. The documents that can be created and edited include spreadsheets, which are called Google Sheets.

viii. *Google Photos*. Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or "exif") data, and can include GPS location information for where a photo or video was taken.

ix. *Google Calendar*. Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered

computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

x. *Google Chats and Google Hangouts content*. Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user's e-mail content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's e-mail and chat content.

xi. *Google Voice*. Google Voice is a telecommunications service provided by Google over the Internet, and can be configured to be used to make phone calls between computers, using voice over IP ("VoIP") connections, or can be configured to be used from existing cellular telephone devices. Google Voice users register Google Voice accounts to an existing Google email account. Users have the ability to configure their Google Voice account to accept calls to an existing landline or cell phone number, or to purchase new telephone numbers, as long as they are available, for a fee from Google. Users can use Google Voice to send or receive SMS messages, commonly referred to as "text messages." A Google Voice user can send a text message from a computer to any cellular telephone, and any text messages which are received by the Google Voice account are available in the user's email inbox, in the account linked to the Google Voice account. Google offers a voicemail service for Google Voice customers. When an incoming call to a Google Voice number is unanswered, the caller may leave a voice message. A copy of the recording, as well as a transcription of the recording are forwarded to the Google Voice user's email account that is linked to the Google Voice account.

xii. *Location History data*. Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

xiii. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

xiv. *Linked Accounts.* Google maintains records of whether the user of an account has other accounts that share the same recovery SMS number or secondary email address. Google also uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways it does that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by Google when a computer visits Google's site or logs into an account.

xv. *Preserved and backup records*. Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving

a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

D. Jurisdiction and Authority to Issue Warrant

5. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

6. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

Overview

8. The U.S. Attorney's Office for the Southern District of New York and IRS-CI are investigating a sophisticated cryptocurrency fraud scheme. The investigation was initiated following public reports in April 2023 that certain individual(s) had executed a multi-step, computer exploit (the "Exploit") that targeted specific cryptocurrency trades on a decentralized

exchange in the period of time between the initial trade request and publication of the trade on the blockchain. Such an attack is believed to be the first of its kind, in that it was designed to exploit the infrastructure of the blockchain. As described below, there is probable cause to believe that two brothers and Massachusetts Institute of Technology ("MIT") graduates, ANTON PERAIRE-BUENO ("Anton") and JAMES PERAIRE-BUENO ("James" and together with Anton, the "Target Subjects"), along with others known and unknown, were involved in the commission of the Subject Offenses. As further described below, there is probable cause to believe that through the Exploit the Target Subjects stole approximately $25 million from at least three victims utilizing at least 60 private cryptocurrency addresses, two virtual network providers, a cryptocurrency privacy protocol service, two foreign-based cryptocurrency exchanges, and multiple bank accounts.

9. This application describes the evidence of the Exploit itself, including several of the core concepts necessary to understand the Exploit, and evidence that the Target Subjects, through the use of the Subject Accounts, designed and executed the Exploit, and thereafter, laundered a large portion of the stolen funds.

A. Probable Cause Regarding the Subject Offenses

The Exploit

10. The Exploit involved a multi-step process that targeted specific cryptocurrency trades on the Ethereum blockchain. Relevant terms and the multi-steps involved in the Exploit are outlined in greater detail below.

11. However, at a high level, to provide context for the terms and steps outlined herein, the Exploit targeted particular victims that specialize in high-frequency cryptocurrency arbitrage trading, which is designed to take advantage of price differences between identical or similar assets in different markets. These victims operated trading bots that identified potential frontrunning

trading opportunities (based on public information) on particular decentralized exchanges. For example, the bots would scan for pending transactions in a particular cryptocurrency that, once executed, would increase the price of that cryptocurrency. The bots would seek to profit from that price increase by submitting a bundled transactions that would consist of the following transactions in the following order: (1) the bots' buy order for the same cryptocurrency whose price it expects to increase; (2) the pending transaction the bots identified that, once executed, increases the price of the cryptocurrency; and (3) the bots' sell order to sell the cryptocurrency it had bought for a profit. Because the bots' buy and sell orders are only valuable if executed in the sequential order just described, the transactions are typically coded with conditions that requires the execution of the trades in that order, or to cancel the bots' buy and sell orders all together.

12. The Exploit can be divided into three phases—preparation, execution, and concealment. In the preparation phase, the hacker(s) initiated a series of trade requests in the months preceding the Exploit that were designed to determine the precise combination of trading parameters most likely to cause the victims' trading bots to trade in a particular manner. In the execution phase, the hacker(s): (i) utilizing the information obtained from the preparation phase transactions, sent transaction requests for specific cryptocurrency trades that the hacker(s) had no intention of executing, but rather, were intended to cause the victims' trading bots to request trades that when executed would affect the prices of particular cryptocurrencies; (ii) gained unauthorized access to the victims' trading requests by sending a false certification; and (iii) once in possession of the private trading data, manipulated that data to the hacker(s) advantage allowing them to unlawfully obtain approximately $25 million. In the concealment phase, the hacker(s) funneled the Exploit fraud proceeds through a series of private cryptocurrency addresses and other blockchain resources to obfuscate the source of the funds.

13. Based on my review of publicly available information, including post-mortem analyses of the Exploit, blockchain scanners, and cryptocurrency publications, along with my training and experience, I have learned the following, in substance and in part, regarding cryptocurrency and cryptocurrency infrastructure as relevant to this investigation:

a. **Cryptocurrency** is digital currency in which transactions are verified and records are maintained by a decentralized system using cryptography, rather than a centralized authority such as a bank or government. Like traditional fiat currency, there are multiple types of cryptocurrency, such as Bitcoin ("BTC") and Ether ("ETH"), among others. Due to its decentralized nature and limited regulation, cryptocurrency allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

b. Cryptocurrency owners typically store their cryptocurrency in digital "**wallets**," which are identified by unique electronic "**addresses**." By maintaining multiple cryptocurrency addresses, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track the flow of illegal proceeds by quickly transferring illicit proceeds in various amounts through multiple cryptocurrency addresses.

c. Each cryptocurrency transaction, regardless of the cryptocurrency denomination, is recorded on a public ledger commonly referred to as a "**blockchain**," which acts as a public accounting ledger. The blockchain records, among other things, the date and time of each cryptocurrency transaction, the unique cryptocurrency addresses associated with the transaction and the sending and receiving parties, and the amount of cryptocurrency transferred, but does not identify the parties that control the cryptocurrency addresses involved in the transaction. Because each cryptocurrency address is unique, law enforcement can review the blockchain to identify relevant cryptocurrency transactions and trace the flow of cryptocurrency across various

cryptocurrency addresses. This form of cryptocurrency tracing is labor intensive and can be complicated by the use of multiple cryptocurrency addresses, and through other commonly used obfuscation techniques, including the use of "cryptocurrency privacy protocols" described later in greater detail. Similar to cryptocurrencies, there are also different types of blockchains, such as Ethereum, Polygon, and BNB Smart Chain. As relevant to this investigation, all criminal activities related to the Subject Offenses occurred on the Ethereum blockchain.

d. "**Blocks**" are data structures within the blockchain database where transaction data in a cryptocurrency blockchain are permanently recorded. Once the data in a proposed block is validated and published to the blockchain, the block is closed. Then, a new block is created for new transactions to be entered into and validated. A block is a permanent store of records that, once written, cannot be altered or removed. Blocks are the fundamental building blocks of a blockchain. The process of validating transactions for a new block, as described in greater detail herein, is essential in ensuring the integrity and security of the blockchain network. As relevant to the Exploit, a block contains transaction data that, once published to the blockchain, is permanently recorded as part of the blockchain's public ledger system. This transparent and previously believed tamper-proof ledger system has transformed the storage and transfer of data. Prior to the Exploit, it was generally considered impossible to tamper with this transparent ledger system. Blocks generally include the following elements:

i. *Blocksize*: Sets the size limit on the block so that only a specific amount of information can be written in it.

ii. *Blockheader*: Contains limited information about the block, such as the rewards a validator may receive for validating the block on the blockchain.

iii. *Transaction counter*: A number that represents how many transactions are stored in the block.

iv. *Transactions*: A list of all transactions within a block.

Blocks are created when a validator, which is described in greater detail below, successfully validates the transactions in the proposed block and publishes the proposed block to the blockchain.

e. "**Block time**" refers to the time separating blocks on the blockchain. On the Ethereum blockchain, time is divided up into 12 second units called "**slots**." In each slot, a single validator is selected to propose a block. One validator is randomly selected to be a block proposer in every slot. This validator is responsible for creating a new block and sending it out to other nodes on the network.

f. A **Decentralized Exchange ("DEX")** is a peer-to-peer marketplace where cryptocurrency transactions occur directly between crypto traders. Unlike centralized exchanges, such as Coinbase or Binance, DEXs do not allow for exchanges between fiat and crypto. Instead, they exclusively trade cryptocurrency tokens for other cryptocurrency tokens. Also unlike centralized exchanges that process various transactions via an "order book" that establishes the price for a particular cryptocurrency based on current buy and sell orders that are matched by an intermediary, commonly referred to as a market maker, DEXs are typically run by smart contracts. While transactions on a centralized exchange are recorded on that exchange's internal database, DEX transactions are normally settled directly on the blockchain. DEXs are usually built on open-source code, which is publicly available.

g. "**Smart contracts**" are computer programs that are stored on a blockchain that automatically run when predetermined conditions are met. They typically are used to automate

the execution of an agreement so that all participants can be immediately certain of the outcome, without an intermediary's involvement or time loss. Once completed, the transactions executed through a smart contract are trackable and irreversible.

h. DEX smart contracts are associated with **liquidity pools** in order to serve as an **automated market maker**. An automated market maker controls a liquidity pool of different types of cryptocurrencies (essentially a pot of money), and uses a smart contract to buy and sell the cryptocurrencies in that liquidity pool. To give an example, an automated market maker smart contract might have a liquidity pool that consisted of 100 ETH and 100 BTC, and that allowed individuals to exchange Ether and Bitcoins. A simple type of automated market maker smart contract would be of the type:

*A (number of cryptocurrency 1) * B (number of cryptocurrency 2) = k (constant).*[2]

In this example, there are 100 ETH (*A*) and 100 BTC (*B*), and the constant (*k*) is 10,000. If an individual wanted to use BTC to purchase 10 ETH from that automated market maker, it would automatically charge a price to maintain the 10,000 constant. In this example, if there were 90 ETH, there would need to be 111.11 BTC in order for the constant to remain the same (90*111.11=10,000). The automated market maker would therefore charge an individual 11.11 BTC for 10 ETH. If there is increased demand for a cryptocurrency, the smart contract will automatically increase the price of that cryptocurrency. In this example, if, after that initial transaction, the person wanted to buy an additional 30 ETH, there would need to be 166.67 BTC in order for the constant to remain the same (60*166.67=10,000). The automated market maker

[2] This simple smart contract is sometimes referred to as the "constant product equation" because the product of the two quantities of cryptocurrencies always remains the same.

would therefore charge an individual 55.56 Bitcoin (166.67 BTC less 111.11 BTC already in the pool) for the additional 30 ETH.

As relevant to the Exploit, the larger the liquidity pool, the less volatile the cryptocurrency prices are. For example, consider a liquidity pool that was one thousand times larger than the previous one, such that there were 100,000 ETH and 100,000 BTC, and therefore a constant of 10,000,000,000. If an individual wanted to purchase 10 ETH from this automated market maker, there would need to be 100,010.001 BTC for the constant to remain the same (99,990*100,010.001 = 10,000,000,000). The automated market maker would therefore charge an individual 10.001 BTC for 10 ETH. By contrast, the smaller the liquidity pool, the more volatile the cryptocurrency prices are, which provides for greater trading arbitrage opportunities.

14. Based on my review of publicly available information, including post-mortem analyses of the Exploit, blockchain scanners, and cryptocurrency publications, along with my training and experience, I have learned the following, in substance and in part, regarding the execution of cryptocurrency transactions on DEXs as relevant to this investigation:

a. When a user conducts a transaction on a blockchain network, such as a buy or sell trade, this transaction is not immediately confirmed. The transaction ultimately has to be validated by a **validator** on proof-of-stake (PoS) blockchains, such as the Ethereum blockchain, who compiles pending transactions into blocks. A transaction is only considered final once it is included in a block that is published to the blockchain. Until then, a transaction will wait in a queue alongside all other unconfirmed transactions in the **memory pool**, which is defined in paragraph 12(c). The time taken to finalize a transaction will depend on a number of factors, including, among others, the particular blockchain network, the time between blocks, network congestion, and **gas fees**.

b. A **gas fee** is the term given to transaction fees on the Ethereum blockchain. Gas is the fee required to successfully execute a transaction on the Ethereum blockchain because it is used to pay validators for validating the pending transactions. Gas fees are priced in tiny fractions of Ether ("ETH"), the cryptocurrency for the Ethereum blockchain. The exact price of the case is determined by supply, demand, and network capacity at the time of a transaction and can be adjusted by the user. Users often pay higher-than-average gas fees and offer tips to incentivize validators to prioritize their transactions.

c. The **memory pool** (**"mempool"**) refers to a backlog of pending and unconfirmed transactions in a blockchain. These unconfirmed transactions wait in the mempool to get validated and finalized in the upcoming block. Pending transactions in the mempool are publicly visible. Pending transactions in the mempool are not processed in a first-come, first-serve process, but rather a searcher, builder, or validator, as described in greater detail below, has the discretion to select transactions to prioritize when creating an upcoming block. Validators are looking to extract the maximum value from a block, often referred to as the maximal extractable value ("MEV"), due to limited blockspace.

d. **MEV** is the maximum profit that a validator can make through their ability to arbitrarily include, exclude, or re-order transactions from the blocks that they propose.

15. Based on my review of publicly available information, including post-mortem analyses of the Exploit, blockchain scanners, and cryptocurrency publications, along with my training and experience, I have learned the following, in substance and in part, regarding MEV-Boost technology as relevant to this investigation:

a. **MEV Boost** is a an open-source software designed to be run by validators to access a competitive block-building market through a system of privacy and commitment protocols.

b. Validators running MEV Boost can maximize their block validating reward by selling block space to specialized third parties called block builders, who collect and sequence transactions to produce a block. In essence, MEV-Boost software is designed to allow validators to outsource the work of finding MEV opportunities in the mempool and building the most profitable block, which in turn, generates the highest profit for the validators.

c. The use of MEV Boost results in the interaction amongst third-parties, including **users**, **searchers, builders,** and **relays**, in the block proposal process as described below:

1. A **user** is a normal Ethereum user who elects to send transactions to a block builder.

2. A **searcher** is a specialized party, such as a trader, that finds profitable transactions and sends them in a "bundle" to a block builder for inclusion in a block. Instead of passing through the public mempool, searcher transactions go to a block builder that orders transactions in a manner designed to maximize MEV. This process encourages transaction privacy.

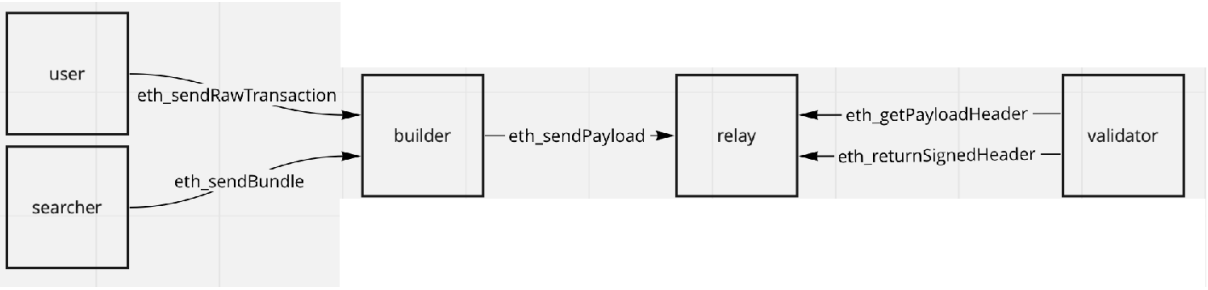
3. A **builder** receives the proposed bundles from searchers who, in addition to the gas fee, express their preferred position in the block by making a sealed-price bid. The builder's job is to build the most profitable block using different strategies. A builder typically invests in specialized hardware necessary for resource-intensive block production. After the builder has compiled the proposed bundles from various searchers into a proposed block that maximizes MEV, it will send the proposed block to a relay, which will ultimately send the proposed block to a validator as described further below.

4. A **validator** is a user selected to propose a block for a particular slot in the blockchain. To participate as a validator, a user must deposit 32 ETH into a deposit contract.

A validator will receive advanced notification when it has been selected to validate a proposed block. Once the proposed block is added to the blockchain, the validator receives transaction fees and MEV tips at a "fee recipient" address specified by the validator.

5. A **relay** is an entity responsible for (i) checking/validating a proposed block before passing it to a validator and (ii) ensuring that the contents of the proposed block remain private until the validator commits to publishing the proposed block as structured by the builder on the blockchain. First, the relay receives the contents of the proposed block from the builder. The relay then transmits the blockheader, which as described above, lists the potential rewards a validator may receive, but does not contain a list of the transactions contained in the proposed block. The validator communicates with the relay to get the most profitable blockheader, which it attests to by signing with its public key. After confirming through its signature with the public key that it will validate the contents of the block as proposed, the relay releases the **execution payload** (*i.e.* – the message containing the lists of transactions to be added to the block) to the validator for validation and block publication.

6. A diagram of the varying participants in the mempool and general sequence of events, moving left to right, involved in executing a cryptocurrency transaction on a DEX using the MEV-Boost system is below:



16. Based on my participation in an interview with the Chief Executive Officer ("CEO") of a victim company ("Victim-1"),[3] as well as my review of publicly available blockchain information, I have learned the following, in substance and in part:

a. Victim-1 is a quantitative trading firm that specializes in high-frequency cryptocurrency arbitrage trading. Such trading activity is designed to take advantage of price differences between identical or similar assets in different markets.

b. Prior to the Exploit, MEV bots owned and controlled by Victim-1 (the "MEV Bots") worked as searchers to identify potential frontrunning trading opportunities[4] on particular DEXs based on publicly available trading data in the mempool.

c. The MEV Bots operated through smart contracts that monitor the mempool to identify profitable trading opportunities based on algorithms and automatically executed those transactions for Victim-1. The algorithms were designed to scan the mempool for profitable frontrunning trading opportunities by identifying pending trades that matched certain pre-identified trading parameters, such as, among others, a set range of gas fees, slippage,[5] and cryptocurrency trades based on market liquidity variables.

[3] Information from Victim-1 has been corroborated in part by other evidence, including documents obtained from Coinbase, Google, and financial institutions in response to grand jury subpoenas, as outlined herein.

[4] "Frontrunning" is the term commonly used to refer to MEV bot trading based on pending transactions in the mempool. Unlike "frontrunning" in the traditional securities context, however, the pending transactions that may create profitable trading opportunities for MEV bots are public and therefore, presumably available for any actor to consider as part of a particular trading strategy.

[5] Slippage refers to the difference between the expected price of a transaction at the time of the trade request and the actual price of a transaction at the time of final execution based on market fluctuation between the request and execution. Like gas fees, a user can set the percentage of slippage the user is willing to accept to execute the transaction.

i. For example, in the instance where a MEV Bot identified a sizeable buy order (the "Attractive Mempool Trade") that, once executed, was expected to increase the price of a particular cryptocurrency, the MEV Bot submitted a bundle to a block builder that contained an ordered transaction list as follows:

MEV Bot Frontrun Trade: Buy request for the same token as pending Attractive Mempool Trade.
Attractive Mempool Trade: Buy request for the particular token.
MEV Bot Backend Trade: Sell request for same taken as Attractive Mempool Trade.

ii. In executing its trades in this fashion, the MEV Bot takes advantage of the price shift likely resulting from the Attractive Mempool Trade by buying moments before the DEX order is executed when the price is lower and then selling shortly after the Attractive Mempool Trade is executed when the sell price is likely higher. The combination of these MEV Bot transactions before (frontrunning) and after (backrunning) to make a profit is often known as "sandwiching" or a "sandwich trade."

iii. Because the MEV Bot bundle is only valuable if executed on the blockchain in sequential order, the computer code typically contains conditions that require the execution of the bundle as ordered or not at all.

d. To protect against being frontrun on their own transactions, Victim-1 elected to use the MEV Boost system, which is available to any DEX user and/or searcher and designed to ensure that the proposed block transactions, including Victim-1's proposed bundles, remain private until

a particular validator commits to publishing the proposed block without any alterations to the list of ordered transactions on the blockchain.

e. On or about April 2, 2023, MEV bots owned and controlled by at least three victims ("Victim-1," "Victim-2," and "Victim-3" and collectively the "Victims") were attacked as part of the Exploit through a code vulnerability in the MEV Boost relay in a series of approximately eight transactions.

f. In particular, the Exploit occurred when a malicious block validator (the "Malicious Validator") sent a false signature (the "False Signature") to the relay. The False Signature was designed to and, in fact, caused the relay to prematurely reveal the full content of the execution payload (*i.e.* – the proposed private trading transactions). The premature publication of this private trading data granted the Malicious Validator a brief period of time to alter certain transactions in the proposed block, which once executed on the blockchain, enabled the Malicious Validator to profit at the Victims' expense.

g. Absent the False Signature, the Malicious Validator would not have received the contents of the proposed block in sufficient time to alter any of the proposed transactions based on the structure of the MEV Boost system.

h. In total, Victim-1 lost approximately $14 million in cryptocurrency and Victims-2 and -3, collectively lost an additional $11 million in cryptocurrency, as a result of the Exploit.[6]

i. Following the Exploit, Victim-1 reviewed publicly available blockchain information prior to the Exploit and identified a series of suspicious transactions beginning in or about February 2023 and continuing up to the day of the Exploit (the "Lure Transactions"). The

[6] Based on my participation in an interview with the CEO of Victim-1, as well as my review of publicly available blockchain information, I have learned that approximately 3 million USDT was frozen by foreign law enforcement shortly after public reports of the Exploit.

Lure Transactions included trade requests with certain characteristics, including, among others, particular slippage parameters and particular cryptocurrency tokens with smaller liquidity pools. The combination of these variables are typically attractive to MEV bots because they generally represent a profitable arbitrage opportunity. Based on Victim-1's review of the Lure Transactions, along with the corresponding trading activity of Victim-1's MEV Bots, it appears that the Lure Transactions were used to determine the combination of trading parameters (*e.g.* – gas fees, slippage, and particular cryptocurrency swaps) that would most likely cause Victim-1's MEV Bots to propose a bundle that included a Lure Transaction.

17. Based on my review of publicly available information, including post-mortem analyses of the Exploit, blockchain scanners, and cryptocurrency publications, along with my training and experience, I have learned the following, in substance and in part, regarding the steps involved in the preparation and execution of the Exploit:

a. As an initial step towards executing the Exploit, the Malicious Validator needed to have the opportunity to validate the bundle containing the Victims' transactions. To become a validator, an Ethereum user must "stake" 32 ETH, which in early 2023 was then equivalent to approximately $55,000.

b. To ensure the maximum profitability of the Exploit, the Malicious Validator also needed to validate a bundle containing particular cryptocurrency transactions involving tokens that the operator of the Malicious Validator already held. In particular, the Exploit appears to have relied upon the Lure Transactions, described above, to predict the trading patterns of the Victims' MEV bots. On or about the day of the Exploit, the hacker(s) deployed particular Lure Transactions (the "Honeypot Transactions") that included trade requests with high slippage parameters for more obscure cryptocurrency tokens, such as Stargate Token ("STG"), Aave Token ("AAVE"), Shiba

Inu ("SHIB"), and Curve DAO Token ("CRV"), that have smaller liquidity pools. The Honeypot Transactions caused the Victims' MEV bots to propose bundles to at least one block builder containing approximately eight sandwich trades that included the Honeypot Transactions as the middle transactions in the manner described above in paragraph 14(c)(i).

c. In order to alter the transactions in the bundles to the advantage of the hacker(s) who operated the Malicious Validator, the Malicious Validator tricked the relay to prematurely release the complete content of the execution payload, including the private trading transactions. The Malicious Validator did this by sending the False Signature to the relay.

d. Once the Malicious Validator was in possession of the private trading transactions, which included the MEV bot sandwich trades based on the Honeypot Transactions, the Malicious Validator replaced the Honeypot Transactions with inverse trades (the "Tampered Transactions") designed to take advantage of the MEV bots' frontrunner transaction, which when executed on the blockchain, would shift the price of the particular cryptocurrency token at issue.

e. On or about April 2, 2023, the Malicious Validator replaced approximately eight Honeypot Transactions in this manner on Block 16964664 (the "Corrupt Block") on the Ethereum blockchain.

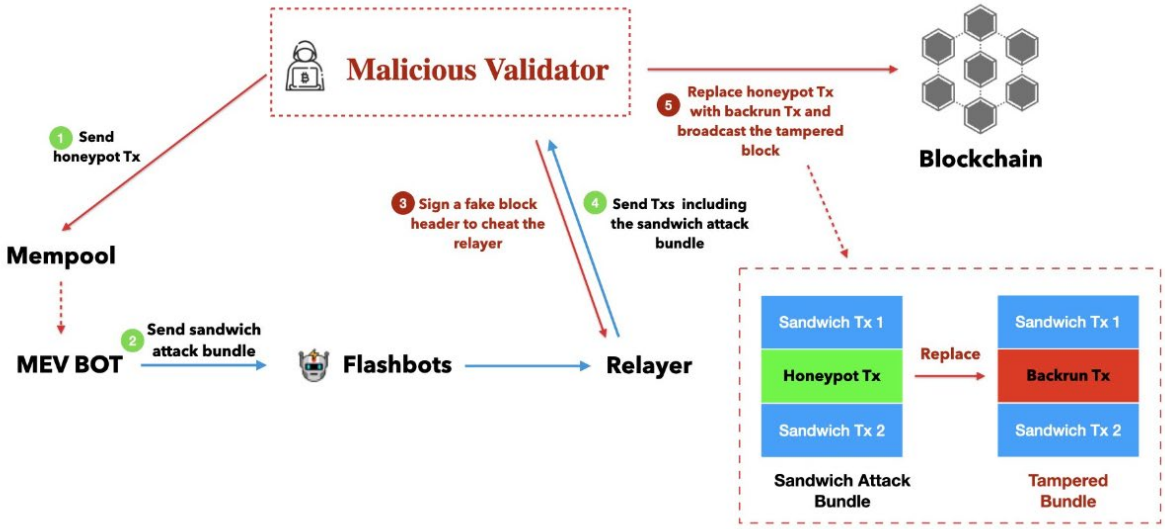
f. An example of one set of transactions from the Corrupt Block, based on Victim-1's MEV Bot activity is outlined below:

Victim-1 Proposed Bundle		**Malicious Validator Tampered Transaction**
MEV Bot Frontrun Trade: *Swap 3,027,389.579264 USDT for 0.089808338417418563 AAVE*		**MEV Bot Frontrun Trade:** *Swap 3,027,389.579264 USDT for 0.089808338417418563 AAVE*
Honeypot Transaction: *Swap 467.738958 USDT for 0.041599288104910821 AAVE*		**Tampered Transaction:** *Swap 1.5630531001469961 83 AAVE for 3,027,396.368333 USDT*
MEV Bot Backend Trade: *Sell AAVE for increased price.*		**MEV Bot Backend Trade:** Failed transaction because there were insufficient funds in the account.

g. Based on my participation in an interview with Victim-1, I learned that Victim-1's frontrun and backrun trades in the proposed bundles should not have been executed on the blockchain if the published block did not contain the Honeypot Transactions, along with the frontrun and backrun trades in sequential order. As a result of the Exploit, however, Victim-1's frontrun trades were executed even though the Corrupt Block did not contain the Honeypot Transactions. Victim-1's backrun trades were not successfully executed because the value of the proposed trade had been captured by the Tampered Transactions.

h. A publicly available diagram of the steps outlined in sub-paragraphs (a)-(d) is outlined below. The diagram was originally published by Blocksec, which based on my training and experience, is a company that specializes in blockchain security research. The diagram

corresponds with the general contours of the Exploit as outlined by Victim-1 and corroborated by publicly available blockchain information:



18. Based on my participation in an interview with a representative of Flashbots, the company that designed the MEV Boost system, as well as my review of publicly available blockchain information, I have learned the following, in substance and in part:

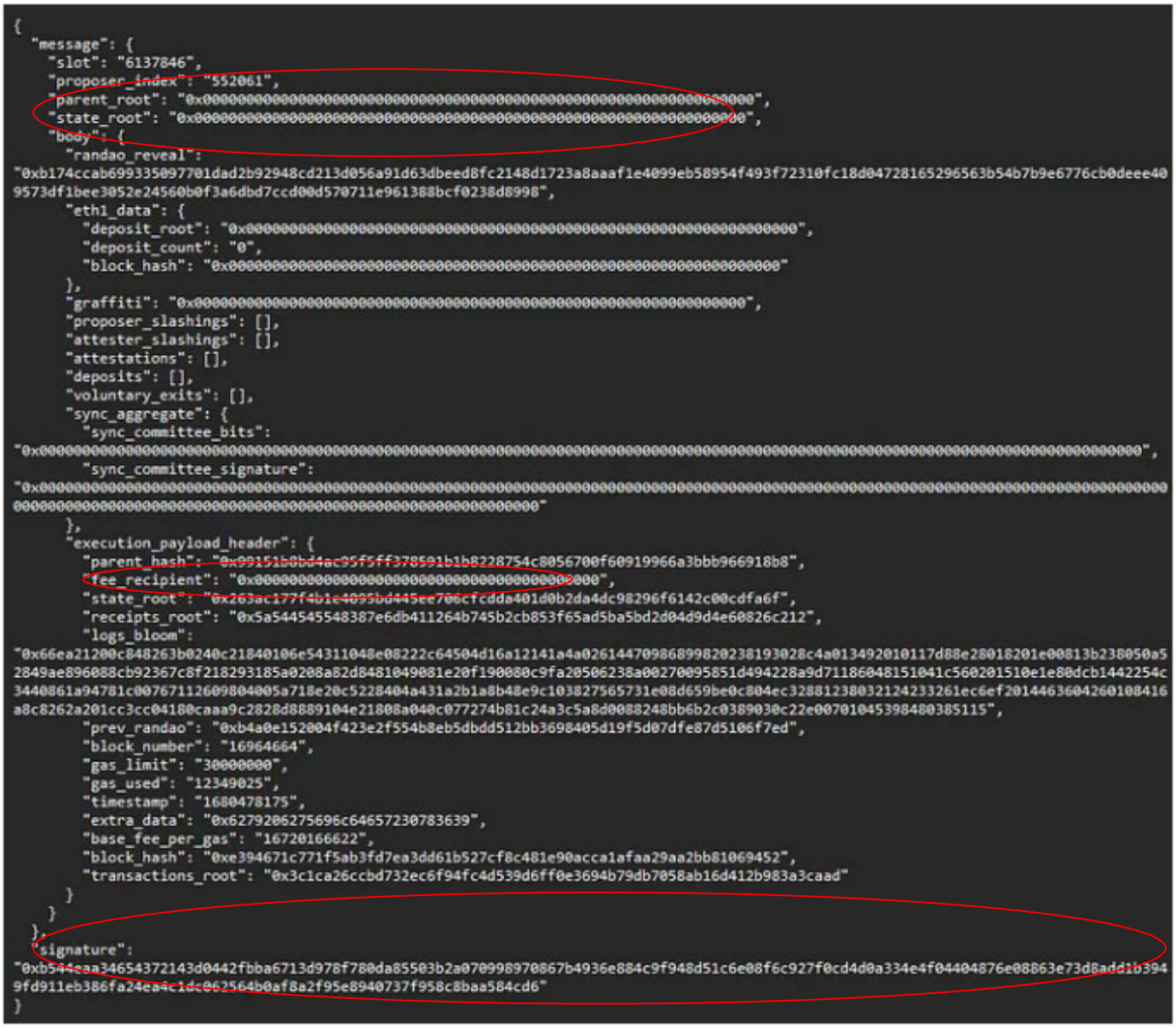
a. The relay is responsible for (i) checking/validating a proposed block before passing it to a validator and (ii) ensuring that the contents of the proposed block remain private until the validator commits to publishing the proposed block as structured by the builder on the blockchain. To ensure the success of both processes, the relay will not release the execution payload (*i.e.* – the message containing the list of transactions to be added to the block) to the validator for validation and block publication until the validator has confirmed through a digital signature that it will publish the proposed block as structured by the builder to the blockchain. Only after confirming the validity of the digital signature will the relay provide a validator with otherwise private trading data.

b. The relay requests a validator's confirmation signature by sending, in the first instance, a blockheader to a validator, which contains basic information about the proposed block, including the proposed block's expected MEV. After reviewing the blockheader, a validator will return the blockheader with a particular signature confirming that the validator will validate and publish the proposed block as structured to the blockchain. Prior to this confirmation signature, a validator will not have access to the otherwise private trading data. In addition to the validator's digital signature, the blockheader also contains other data fields that are populated with information provided by a validator, among others, at various points in MEV Boost process. These data fields are used by particular Ethereum actors to determine whether the proposed block contains appropriate criteria to be published to the blockchain.

c. The Exploit hacker(s) targeted the blockheader exchange between the relay and the validator as an essential part of the Exploit.

[INTENTIONALLY LEFT BLANK]

d. A publicly available screenshot of the computer code from the blockheader for the Corrupt Block containing the False Signature is shown below:



{
  "message": {
    "slot": "6137846",
    "proposer_index": "552061",
    "parent_root": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "state_root": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "body": {
      "randao_reveal":
"0xb174ccab699335097701dad2b92948cd213d056a91d63dbeed8fc2148d1723a8aaaf1e4099eb58954f493f72310fc18d04728165296563b54b7b9e6776cb0deee40
9573df1bee3052e24560b0f3a6dbd7ccd00d570711e961388bcf0238d8998",
      "eth1_data": {
        "deposit_root": "0x0000000000000000000000000000000000000000000000000000000000000000",
        "deposit_count": "0",
        "block_hash": "0x0000000000000000000000000000000000000000000000000000000000000000"
      },
      "graffiti": "0x0000000000000000000000000000000000000000000000000000000000000000",
      "proposer_slashings": [],
      "attester_slashings": [],
      "attestations": [],
      "deposits": [],
      "voluntary_exits": [],
      "sync_aggregate": {
        "sync_committee_bits":
"0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",
        "sync_committee_signature":
"0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000"
      },
      "execution_payload_header": {
        "parent_hash": "0x0015b0bd4ac95f5ff378591b1b8228754c8056700f60919966a3bbb966918b8",
        "fee_recipient": "0x0000000000000000000000000000000000000000",
        "state_root": "0x263ac177f4b1e4055bd445ee700cfcdda401d0b2da4dc98296f6142c00cdfa6f",
        "receipts_root": "0x5a544545548387e6db411264b745b2cb853f65ad5ba5bd2d04d9d4e60826c212",
        "logs_bloom":
"0x66ea21200c848263b0240c21840106e54311048e08222c64504d16a12141a4a026144709868998202381930028c4a013492010117d88e28018201e00813b238050a5
2849ae896088cb92367c8f218293185a0208a82d8481049081e20f190080c9fa2050623 8a0027009585 1d494228a9d7118604815 1041c560201510e1e80dcb1442254c
3440861a94781c00767112609804005a718e20c5228404a431a2b1a8b48e9c103827565731e08d659be0c804ec32881238032124233261ec6ef2014463604260108416
a8c8262a201cc3cc04180caaa9c2828d8889104e21808a040c077274b81c24a3c5a8d0088248bb6b2c0389030c22e0070104539848038 5115",
        "prev_randao": "0xb4a0e152004f423e2f554b8eb5dbdd512bb3698405d19f5d07dfe87d5106f7ed",
        "block_number": "16964664",
        "gas_limit": "30000000",
        "gas_used": "12349025",
        "timestamp": "1680478175",
        "extra_data": "0x6279206275696c64657230783639",
        "base_fee_per_gas": "16720166622",
        "block_hash": "0xe394671c771f5ab3fd7ea3dd61b527cf8c481e90acca1afaa29aa2bb81069452",
        "transactions_root": "0x3c1ca26ccbd732ec6f94fc4d539d6ff0e3694b79db7058ab16d412b983a3caad"
      }
    }
  },
  "signature":
"0xb541eaa34654372143d0442fbba6713d978f780da85503b2a070998970867b4936e884c9f948d51c6e08f6c927f0cd4d0a334e4f04404876e08863e73d8add1b394
9fd911eb386fa24ea4c1dc062564b0af8a2f95e8940737f958c8baa584cd6"
}

e. By providing a valid public key signature, as seen in the "signature" field, but setting the parent and state roots to a series of zeros as highlighted in one of the red circles above, the False Signature caused the relay code to incorrectly verify that the blockheader had been validly signed, but in fact, the proposed block had no chance to be approved for publication to the

blockchain. The False Signature caused the relay to prematurely release the execution payload—including the private trading transaction data—to the Malicious Validator. Once in possession of the execution payload, the Malicious Validator altered certain transactions in the proposed block. Thereafter, the Malicious Validator resubmitted the proposed block with the Tampered Transactions that was published to the blockchain.

f. As an additional step in the Exploit, the hacker(s) also set the Malicious Validator's fee recipient address as highlighted in one of the red circles above —the address used by a validator to receive fees for publishing a proposed block to the blockchain—to a series of zeros, which is an invalid cryptocurrency address. These fees are the typical way that validators make money from validating cryptocurrency transactions. Based on my training and experience, I believe that the hacker(s) set the fee recipient address to zeros, which effectively destroyed any chance of the Malicious Validator receiving fees from the tampered validation process, to minimize the number of cryptocurrency addresses that could be traced back to the hacker(s).

g. As outlined above, when a validator fails to perform its validation task correctly, it may be penalized by other Ethereum users who have the ability to "slash" one ETH from the validator's 32 staked ETH. Because the Malicious Validator improperly signed the Corrupt Block by sending the False Signature, it was slashed one ETH by another Ethereum user.

19. Based on the foregoing, there is probable cause to believe that the hacker(s) (i) sent requests for trades that they had no intention of executing (*e.g.* the Honeypot Transactions) in order to manipulate the prices of particular cryptocurrencies, and thereafter, (ii) sent false information to the relay *(e.g.* the False Signature) to receive otherwise private trading data. Once in possession of this private trading data, the hacker(s) deliberately altered certain transactions, which once

executed, resulted in approximately $25 million in fraudulent profit, in violation of the Subject Offenses.

B. Probable Cause Regarding the Subject Accounts

Identification of the Target Subjects and the Subject Accounts

20. The successful execution of the Exploit required multi-steps, including the creation of at least 16 validators and the transfer of the fraud proceeds through numerous accounts. As outlined in greater detail below, the Target Subjects are linked to the Exploit primarily through a particular Coinbase account, identified below as the Pine Needle Coinbase Account, which was used (i) to fund the creation of the validators, including the Malicious Validator, prior to the Exploit, (ii) to receive the return of the validator staking fees, including the Malicious Validator's slashed staking fees, after the Exploit, and (iii) to receive and transfer the Exploit fraud proceeds. In addition, the Target Subjects are linked to the Exploit through matching and/or Internet Protocol ("IP") addresses as outlined in greater detail below.

21. Based on my review of publicly available blockchain information, I have learned the following, in substance and in part, with respect to the Malicious Validator:

a. Each validator is assigned a unique identifying index number that is publicly visible on blockchain records. The Malicious Validator was assigned a particular index number (the "Malicious Validator Index Number").

b. Publicly available identifying details linked to the Malicious Validator Index Number establish that the Malicious Validator was originally funded by a particular cryptocurrency address (the "Malicious Validator Funding Address") on or about March 15, 2023, *i.e.*, approximately two weeks before the Exploit.

c. On or about October 5, 2023, the Malicious Validator Funding Address sent approximately 31.0381 ETH to a particular Coinbase account outlined in detail below (the "Pine

Needle Coinbase Account"). As discussed above, a validator must stake 32 ETH to become a validator on the Ethereum blockchain. Based on my review of the blockchain, 31 ETH is consistent with the fact that the Malicious Validator was slashed one ETH for improperly signing the Corrupt Block as described in paragraph 18(g).

22. Based on my review of records provided by Coinbase, as well as publicly available blockchain information, I have learned the following, in substance and in part:

a. The Pine Needle Coinbase Account was created on or about February 5, 2023.

b. The Pine Needle Coinbase Account is registered to the business "Pine Needle Inc." on behalf of "Anton Peraire-Bueno" with the email address anton-pine-needle@18decimal.io (**Subject Account-1)**.

c. Between on or about March 2, 2023 and March 20, 2023 (*i.e.*, in the weeks leading up to the Exploit), 14 intermediary cryptocurrency addresses received approximately 505 ETH directly from the Pine Needle Coinbase Account in a series of transactions (collectively, the "Intermediary Addresses"). Between on or about February 28, 2023 and March 6, 2023, through a series transactions involving Bybit, a foreign cryptocurrency exchange, two of the Intermediary Addresses also received approximately 24.5 ETH indirectly from the Pine Needle Coinbase Account.

d. In total, between on or about February 28, 2023 and on or about March 20, 2023, the Pine Needle Coinbase Account sent approximately 529.5 ETH to the Intermediary Addresses either directly or indirectly. After March 20, 2023, the Intermediary Addresses have no further incoming or outgoing transactions. Based on my training and experience, the fact that the Intermediary addresses have no further incoming or outgoing transaction activity based on public

blockchain records suggests that the Intermediary Addresses were used to obfuscate the connection between the Pine Needle Coinbase Account and the execution of the Exploit.

e. On or about March 2, 2023 and March 20, 2023—before the Exploit, the Intermediary Addresses sent approximately 529.5 ETH (*i.e.*, the same amount that the Pine Needle Coinbase Account sent to the Intermediary Addresses) to the Aztec Network in a series of transactions ranging in dates and amounts. Based on my training and experience, I known that the Aztec Network is a privacy layer for the Ethereum blockchain that offers users the ability to conceal certain information about the sender and/or receiver of a transaction. As outlined in greater detail below, 529.5 ETH is a sufficient amount to fund the creation of 16 validators, each staked by 32 ETH.

f. Between on or about May 30, 2023 and on or about June 12, 2023—after the Exploit, the Pine Needle Coinbase Account received approximately 480 ETH in a series of 15 transactions, each totaling approximately 32 ETH. Each of the 15 transactions contained a unique "from" transaction hash that identified the sender address (collectively, the "Validator Addresses").

g. Based on my review of the Validator Addresses on the blockchain, I learned that each Validator Address received multiple transactions from the Aztec Network either directly or indirectly between on or about March 3, 2023 and on or about March 15, 2023 that totaled approximately 32 ETH per Validator Address. During the same time period, the Validator Addresses then sent their respective 32 ETH to a particular smart contract to become a validator.

h. Based on my review of the Malicious Validator Funding Address on the blockchain, I learned that on or about March 15, 2023, the Malicious Validator Funding Address also received multiple tranfers from the Aztec Network, totaling approximately 32.036 ETH.

i. Based on the foregoing, between on or about February 28, 2023 and March 20, 2023—before the Exploit, the Pine Needle Coinbase Account appears to have funded the creation of 16 different validators through the Aztec Network, costing approximately $880,000 in cryptocurrency. By creating 16 validators, the Target Subjects increased the probability that their validator would be selected from the pool of thousands of validators. Following the Exploit, between on or about May 30, 2023 and on or about October 5, 2023, the Pine Needle Coinbase Account received approximately 511 ETH, representing 32 ETH from 15 Validator Addresses and 31 ETH from the Malicious Validator Funding Address.

j. Between on or about May 30, 2023 and on or about October 5, 2023, the Pine Needle Coinbase Account also transferred approximately $998,118 to a particular bank account (the "Pine Needle Bank Account") in a series of transactions that were each correlated within days of when a particular Validator's staking fees (*i.e.* 32 ETH) were returned to the Pine Needle Coinbase Account.

k. On or about October 18, 2023, a particular Internet protocol ("IP") address—185.153.177.164 (the "Pine Needle Coinbase Account IP Address")—was used to login to the Pine Needle Coinbase Account and transfer funds to the Pine Needle Bank Account.

23. Based on my review of publicly available blockchain information, I have learned the following, in substance and in part:

a. On or about April 2, 2023, the Malicious Validator altered approximately eight transactions on the Corrupt Block as part of the Exploit. The Exploit fraud proceeds, totaling approximately $25 million in various cryptocurrencies (the "Exploit Fraud Proceeds"), were deposited into eight separate addresses (the "Exploit Addresses"), which were initially funded between on or about February 27, 2023 and on or about March 13, 2023, through KuCoin, a

particular foreign cryptocurrency exchange. Shortly thereafter, the Exploit Addresses converted the various cryptocurrencies comprising the Exploit Fraud Proceeds to less-volatile stablecoins, including, among others, DAI.[7]

b. Between on or about April 3, 2023 and on or about April 6, 2023, the Exploit Addresses transferred approximately $25 million the Exploit Fraud Proceeds to a particular address identified by a unique transaction hash and publicly identified on the blockchain as the "Low Carb Crusader" (the "Low Carb Crusader Address"). Based on my training and experience, I believe that the title "Low Carb Crusader" is a reference to the fact that the Exploit targeted MEV bots executing "sandwich trades."

i. The Low Carb Crusader Address is a smart contract that can receive and send cryptocurrency. The publicly available smart contract code identifies seven different cryptocurrency address as the owners of the Low Carb Crusader Address. Based on my training and experience, I know that the owner(s) of a smart contract are typically the only users authorized to execute call functions (*i.e.* - commands for the smart contract to perform, such as an automated transfer of funds). As relevant to the Exploit, one of the seven owner addresses (the "Low Carb Crusader Owner Address") was responsible for the execution of the majority of the Low Carb Crusader Address's call functions.

ii. The Low Carb Crusader Address was funded on or about March 25, 2023 with a nominal amount of ETH.

iii. Prior to the receipt of the Exploit Fraud Proceeds, the Low Carb Crusader Address had an account balance of less than approximately $1,000 in cryptocurrency.

[7] Based on my training and experience, I know that stablecoins are digital currencies whose value is pegged, or tied to that of another currency, commodity, or financial instrument such as the U.S. dollar or gold to maintain a stable value.

c. Between on or about September 2, 2023 and on or about October 26, 2023, in a series of transactions, the Low Carb Crusader Address sent approximately $20,472,567 in DAI, representing a large portion of the Exploit Fraud Proceeds to the MakerDAO.[8] The MakerDAO is smart contract that operates as a decentralized global reserve bank that resides on the Ethereum blockchain that permits individuals to borrow and/or lend DAI.

d. Between on or about October 15, 2023 and on or about October 16, 2023, the Pine Needle Coinbase Account engaged in a series of transactions that permitted the account to receive the Exploit Fraud Proceeds back from the MakerDAO. In particular, on or about October 15, 2023, the Pine Needle Coinbase Account funded a particular cryptocurrency address, which was used on or about October 16, 2023, to create a smart contract (the "MakerDAO Contract") that appears to have been used to receive the Exploit Fraud Proceeds back from the MakerDAO. Between on or about October 16, 2023 and on or about November 20, 2023, through a series of approximately 16 transactions, the MakerDAO Contract received approximately 20,516,758 DAI from the MakerDAO. During this same period, the MarkerDAO Contract swapped approximately 20,516,758 DAI for approximately 20,516,758 USDC, which was then deposited into the Pine Needle Coinbase Account from the MakerDAO Contract.

e. Based on my training and experience, I believe that this series of multiple cryptocurrency transfers to and from private addresses and through the MakerDAO was used primarily, if not exclusively, for money laundering purposes to obfuscate the source of the Exploit Fraud Proceeds.

[8] As described in footnote 7, foreign law enforcement froze approximately 3 million USDT shortly after the Exploit, which remains frozen in the Low Carb Crusader Address and publicly visible on the blockchain.

f. Based on my review of the Pine Needle Coinbase Account records from on or about February 9, 2023 to on or about October 15, 2023, prior to the receipt of the Exploit Fraud Proceeds, the Pine Needle Coinbase Account balance did not exceed approximately $2.1 million in cryptocurrency.

24. A visual representation of the flow of funds prior to and after the Exploit, beginning with the transfer of funds from the Pine Needle Coinbase Account to the Intermediary Addresses; then to the Aztec Network to fund the creation of the Validators, including the Malicious Validator; and ultimately, back to the Pine Needle Coinbase Account with the Exploit Fraud Proceeds and returned Validator staking fees is outlined in **Appendix 1**, attached hereto.

25. Based on my review of records provided by Mercury Bank, I have learned the following, in substance and in part:

a. The Pine Needle Bank Account consists of both a checking and savings account, which was created on or about January 4, 2023.

b. The Pine Needle Bank Account is registered to "Anton Peraire-Bueno" at anton-pine-needle@18decimal.io (**Subject Account-1**) and "James Peraire-Bueno" at james-pine-needle@18decimal.io (**Subject Account-2**).

c. Between on or about October 16, 2023 and on or about November 20, 2023, the Pine Needle Coinbase Account transferred approximately $20,516,758, representing the Exploit Fraud Proceeds, to the Pine Needle Bank Account.

d. On or about October 18, 2023, the Pine Needle Coinbase Account IP Address was used to login to the Pine Needle Bank Account.

e. On or about October 23, 2023, the Pine Needle Bank Account transferred approximately $20,481,431 to another Mercury Bank account in the named "Birch Bark Trading LLC" (the "Birch Bark Bank Account").

f. The Birch Bark Bank Account is also registered to "Anton Peraire-Bueno" at anton@18decimal.io (**Subject Account-3**) and "James Peraire-Bueno" at james@18decimal.io (**Subject Account-4**).

g. The Birch Bark Bank Account was created on or about September 21, 2023.

h. Between on or about October 20, 2023 and on or about October 23, 2023, a representative from Mercury Bank emailed Anton at **Subject Account-1** and **Subject Account-3** and inquired about the relationship between Pine Needle Inc. and Birch Bark Trading LLC and the source of the approximately $20,481,431 deposited into the Pine Needle Bank Account, which was transferred to the Birch Bark Bank Account. Anton responded, in sum and substance, as follows:

i. The more than $20 million deposited into the Pine Needle Bank Account represented "capital gains for Birch Bark resulting from on-chain transactions."

ii. Anton provided Mercury Bank with an excerpt of a service agreement between Pine Needle Inc. and Birch Bark Trading LLC. The service agreement effective "January 1, 2023" claimed that Pine Needle Inc. was a "service provider" for Birch Bark Trading LLC that provided "software development services," including running "Ethereum Validators."

26. Based on my review of records provided by the State of Wyoming Office of the Secretary of State, I have learned the following, in substance and in part:

a. Pine Needle Inc. is registered to James, as, among other titles, the Treasurer, and Anton, as, among other titles, the President, and was incorporated on or about December 28, 2022.

27. Based on my review of records provided by the State of Delaware, I have learned the following, in substance and in part:

a. Birch Bark Trading LLC was incorporated on or about March 7, 2023.

b. Birch Bark Trading LLC is registered to The Corporation Trust Company, a registered agent.

28. Based on my review of records provided by the Commonwealth of Massachusetts, I have learned the following, in substance and in part:

a. The domain "18decimal.io," which is included as part of the email addresses for Subject Accounts-1 through -4, appears to be a reference to the business entity "18Decimal Inc."

b. 18Decimal Inc. is registered to James, as, the Treasurer, Secretary, and Director, and Anton, as, the President and Director, and was incorporated on or about November 16, 2021.

29. Based on my review of records provided by Google, I have learned the following, in substance and in part:

a. **Subject Account-1** is an alias for **Subject Account-3**. As described above in paragraph 4(b)(i), an alias address is an alternate email address that is linked to an individual's primary email address. Messages sent to an alias address are delivered to the primary email address, which in this case is **Subject Account-3**. **Subject Account-1** was created on or about at least November 3, 2021 and remains active. **Subject Account-1** is registered to "Anton Peraire-Bueno." **Subject Account-1** uses the following Google services, among others, Gmail, Google Hangouts, Google Chat, Google Docs, Google Drive, and Apps Script.

b. The recovery email address for **Subject Account-1** is antonperairebueno2000@gmail.com (**Subject Account-5**). Based on my training and experience, in choosing a recovery email address, individuals typically use a second email account that they

control completely. Among other reasons, this ensures security for the underlying account because when a user forgets a password, his only ability to regain access is typically to ask an email provider to send information to a recovery email address. If a user registered a recovery email address that was controlled by another person, that second person could obtain exclusive control of the primary email at the expense of the first person. According, based on my training and experience in investigations of computer crimes, I believe that **Subject Account-5** is controlled by the same individual who controls **Subject Account-1**.

c. **Subject Account-2** is an alias account for **Subject Account-4**. **Subject Account-2** was created on or about at least November 3, 2021 and remains active. **Subject Account-2** is registered to "James Peraire-Bueno." **Subject Account-2** uses the following Google services, among others, Gmail, Google Hangouts, Google Chat, Google Docs, Google Drive, and Apps Script.

d. The recovery email address for **Subject Account-2** is jamesperairbueno@gmail.com (**Subject Account-6**). Based on the reasoning described in paragraph 29(b), I believe that **Subject Account-6** is controlled by the same individual who controls **Subject Account-2**.

e. **Subject Account-3** was created on or about November 3, 2021 and remains active. **Subject Account-3** is registered to "Anton Peraire-Bueno." The recovery email address for **Subject Account-3** is **Subject Account-5**. **Subject Account-3** uses the following Google services, among others, Gmail, Google Hangouts, Google Chat, Google Docs, Google Drive, and

Apps Script. As relevant to this application, **Subject Account-3** utilized the Internet Protocol ("IP")[9] Address outlined below on the listed dates to login **Subject Account-3**:

Timestamp	IP Address
2023-09-05 16:31:09	179.48.248.13 (the "Data Miners IP Address")

f. **Subject Account-4** was created on or about November 3, 2021 and remains active. **Subject Account-4** is registered to "James Peraire-Bueno." The recovery email address for **Subject Account-4** is **Subject Account-6**.[10] **Subject Account-4** uses the following Google services, among others, Gmail, Google Hangouts, Google Chat, Google Docs, Google Drive, and Apps Script.

g. **Subject Account-5** was created on or about November 3, 2013 and remains active. **Subject Account-5** is registered to "Anton PB." **Subject Account-5** uses the following Google services, among others, Gmail, Google Photos, Google Hangouts, Google Drive, and Google Docs. As relevant to this application, **Subject Account-5** utilized the IP Addresses outlined below on the listed dates to login **Subject Account-5**:

Timestamp	IP Address
2023-02-03 20:38:21	185.153.177.59 (the "Nord VPN IP Address")

[9] Based on my training and experience, I know that an IP address is a unique string of characters assigned by an internet service provider ("ISP") to Internet-connected devices for the purposes of communicating over a network. It is possible for two or more electronic devices to share an IP address if these devices access the internet from a local network ("LAN")—essentially, while users may be using different computers or devices in one location, if these devices are all using the same internet connection, they will share an IP address.

2023-02-12 14:04:20	192.154.196.249 (the "Vivid Hosting IP Address")

h. **Subject Account-6** was created on or about June 26, 2010 and remains active. **Subject Account-6** is registered to "James Peraire." **Subject Account-6** uses the following Google services, among others, Gmail, Google Hangouts, Google Docs, Google Photos, Google Drive, and Google Payment.

30. Based on my review of publicly available ISP registry directories, I have learned the following, in substance and in part:

a. The Data Miners IP Address is hosted by Data Miners S.A., which is a virtual private network ("VPN") service provider. Based on my training and experience, I know that a VPN enables a user to send and receive data across an encrypted network that conceals a user's true IP address.

b. The Nord VPN IP Address is hosted by Tefincom S.A. (d/b/a Nord VPN), which is a VPN service provider.

c. The Vivid Hosting IP address is hosted by Vivid-Hosting LLC, which is a VPN service provider.

d. Based on my training and experience, I know that the Registry for Internet Numbers is the authority for assigning IP addresses, which can range from 0.0.0.0 to 255.255.255.255. The Registry for Internet Numbers typically assigns IP addresses in a net range to ISPs (*e.g.* 179.48.248.0 to 179.48.251.255). The net range for the relevant ISP providers are as follows:

ISP	**ISP Net Range**
Data Miners S.A	179.48.248.0 - 179.48.251.255

Nord VPN	185.153.177.0 - 185.153.177.255
Vivid-Hosting LLC	192.154.192.0 – 192.154.223.255

31. Based on my review of records provided by Paraswap and Coinbase, and publicly available information, including blockchain transaction records, along with my training and experience, I have learned the following, in substance and in part:

a. Paraswap is a DEX that allows users to trade various cryptocurrency denominations.

b. Between on or about August 28, 2023 and on or about September 18, 2023, the Low Carb Crusader Address used Paraswap to trade cryptocurrency in a series of transactions. During this period of time, Paraswap captured three IP addresses that were used by the Low Carb Crusader Address when it interacted with Paraswap as follows:

i. 179.48.248.13 (the Data Miners IP Address)

ii. 185.153.177.154 (the Nord VPN IP Address)

iii. 192.154.196.239 (the Vivid Hosting VPN IP Address)

c. On or about October 18, 2023, the Low Carb Crusader Owner Address interacted with Paraswap to trade cryptocurrency. Paraswap captured a particular IP address—185.153.177.164—that was used by the Low Carb Crusader Owner Address when it interacted with Paraswap.

d. Based on my comparison of the Pine Needle Coinbase Account's, **Subject Account-3**'s, and **Subject Account-5**'s IP addresses with the Paraswap records, I know the following:

i. The Data Miner IP Address was used to login to **Subject Account-3** on or about September 5, 2023, and to transact with Paraswap from the Low Carb Crusader Address on or about September 18, 2023.

ii. The Nord VPN IP Address that was used to login to **Subject Account-5** on or about February 3, 2023, belongs to the same Nord VPN range that was used by (i) the Low Carb Crusader Address to interact with Paraswap on or about September 18, 2023, (ii) the Low Carb Crusader Owner Address to interact with Paraswap on or about October 18, 2023, (iii) the Pine Needle Coinbase Account on or about October 18, 2023, and (iv) the Pine Needle Bank Account on or about October 18, 2023.

iii. The Vivid Hosting IP Address that was used to login to **Subject Account-5** on or about February 12, 2023, belongs to the same Vivid Hosting LLC range that was used by the Low Carb Crusader Address to interact with Paraswap on or about September 18, 2023.

32. Based on the foregoing, there is probable cause to believe that the Subject Accounts will contain evidence of the user(s) of the Subject Accounts; the transfer of funds through the Pine Needle Coinbase Account, the Pine Needle Bank Account, and the Birch Bark Bank Accounts; and actions taken to prepare for, execute, and thereafter, conceal the Exploit. Law enforcement has served preservation requests on the Provider pursuant to 18 U.S.C. § 2703(f)(1) requiring the Provider to preserve content information associated with the Subject Accounts for a period of 90 days. Specifically, law enforcement served preservation requests on the Provider for Subject Account-1, -4, and -5 on or about October 19, 2023, Subject Accounts-2 and -3 on or about November 22, 2023, and Subject Account-6 on or about December 17, 2023 (Ref. Nos. 45076307, 47398959, and 49064137).

33. Temporal Limitation. This application is limited to all content created, sent, deleted, or received on or after July 1, 2022 through the date of this application, inclusive. As described above, accounts and transactions related to the Exploit were taken as early as February 2023. Due to the sophisticated nature of the Exploit, there is reason to believe that the Target Subjects began planning the Exploit several months prior to the first cryptocurrency transactions. The July 1, 2022 limitation date provides for a limited period of time prior to these transactions to capture any content created, sent, or received related to the Subject Offenses, which was generated in preparation of the Exploit.

C. Evidence, Fruits and Instrumentalities

34. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers' servers associated with the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

a. Evidence sufficient to establish the user(s) of the Subject Accounts at times relevant to the Subject Offenses, including photographs, contact information, payment information, and other personally identifiable information.

b. Evidence sufficient to establish the user(s) of various bank accounts and cryptocurrency accounts containing the names "Pine Needle," "Birch Bark," and "18decimal."

c. Evidence concerning the planning of the MEV-boost relay computer exploit on or about April 2, 2023 (the "Exploit"), including research regarding, among other things, the operation of decentralized exchanges ("DEXs"), MEV-boost relay system, and various ways to obscure cryptocurrency transactions, and purchases of various items including, among other things, technology to obscure identification details.

d. Evidence of statements, representations, and omissions made by ANTON PERAIRE-BUENO ("Anton"), JAMES PERAIRE-BUENO ("James"), and other co-conspirators concerning the preparation, execution, and concealment of the Exploit.

e. Evidence of computer code concerning the Exploit.

f. Evidence concerning Anton and James trading strategies and use of MEV Bots.

g. Evidence of knowledge by Anton and James concerning the purpose of the Exploit, including the ability to lure particular MEV bots to certain transactions and obtain access to private trading data.

h. Evidence of concealment of the Exploit and the funds obtained from the Exploit.

i. Evidence of unlawful agreements, including to commit fraud, misappropriate commodities transactions, gain unauthorized computer access, and/or engage in money laundering.

j. Evidence establishing the relationship amongst Anton, James, and/or any other co-conspirators.

k. Evidence of the receipt, transfer, disposition, or location of funds raised through the commission of the Subject Offenses.

l. Evidence of efforts to conceal the commission of the Subject Offenses and evade detection by law enforcement and/or regulatory agencies.

m. Evidence of the geographic location of the users of the Subject Accounts.

n. Evidence of passwords or other information needed to access the Subject Accounts or other accounts of the users of the Subject Accounts.

o. Evidence relating to other accounts, devices, or physical premises in which evidence of the commission of the Subject Offenses may be found.

III. Review of the Information Obtained Pursuant to the Warrant

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

36. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently

there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

37. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. Here, the investigation involves internet infrastructure and electronic evidence that could be tampered with or destroyed. Additionally, the Target Subjects of the investigation have significant financial resources. Premature disclosure to the subjects of the investigation could give them insights about the direction of the investigation, causing them to flee or destroy evidence.

38. Accordingly, there is reason to believe that, were the Provider to notify specific account holders or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

39. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V.Conclusion

40. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

/s/ Marco Dias, with permission
MARCO DIAS
Special Agent
Internal Revenue Service-Criminal Investigation

Sworn to me through the transmission of this Affidavit by reliable electronic means, pursuant to Federal Rules of Criminal Procedure 41(d)(3) and 4.1, this 5th day of January, 2024

JAMES L. COTT
United States Magistrate Judge

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with Six Email Accounts Maintained at Premises Controlled by Google, LLC, USAO Reference No. 2022R00863

24 MAG 56

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, LLC ("Provider")

Internal Revenue Service-Criminal Investigation ("Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent Marco Dias of Internal Revenue Service-Criminal Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts specified in Attachment A, maintained at premises controlled by Google, LLC contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, and/or flight from

prosecution, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

01/05/2024 11:43 AM

Date Issued Time Issued

JAMES L. COTT
United States Magistrate Judge

Email Search Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Google, LLC (the "Provider"), and applies to all content and other information within the Provider's possession, custody, or control associated with the email accounts specified below:

antonperairebueno2000@gmail.com
anton-pine-needle@18decimal.io
james-pine-needle@18decimal.io
anton@18decimal.io
james@18decimal.io
jamesperairebueno@gmail.com

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Google. Google is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts specified above, limited to all content created, sent, deleted, or received on or after July 1, 2022 through the date of this warrant, inclusive:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header

information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email)

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information*. All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records*. All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Document Management.* All Google Drives associated with the Subject Accounts.

g. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including but not limited to Google reference numbers: 45076307, 47398959, and 49064137.

III.Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of a cryptocurrency fraud scheme, involving a computer exploit, in or about

April 2023, in violation of wire fraud and conspiracy to commit wire fraud, 18 U.S.C. § 1343 and 1349; computer fraud, 18 U.S.C. § 1030; commodities fraud and conspiracy to commit commodities fraud, 18 U.S.C. § 371, 7 U.S.C. § 9(1) and 13(a)(5), and 17 C.F.R. § 180.1; commodities fraud manipulation, 7 U.S.C. § 13(a)(2); and money laundering and conspiracy to commit money laundering, 18 U.S.C. §§ 1956 and 1957, including the following:

a. Evidence sufficient to establish the user(s) of the Subject Accounts at times relevant to the Subject Offenses, including photographs, contact information, payment information, and other personally identifiable information.

b. Evidence sufficient to establish the user(s) of various bank accounts and cryptocurrency accounts containing the names "Pine Needle," "Birch Bark," and "18decimal."

c. Evidence concerning the planning of the MEV-boost relay computer exploit on or about April 2, 2023 (the "Exploit"), including research regarding, among other things, the operation of decentralized exchanges ("DEXs"), MEV-boost relay system, and various ways to obscure cryptocurrency transactions, and purchases of various items including, among other things, technology to obscure identification details.

d. Evidence of statements, representations, and omissions made by ANTON PERAIRE-BUENO ("Anton"), JAMES PERAIRE-BUENO ("James"), and other co-conspirators concerning the preparation, execution, and concealment of the Exploit.

e. Evidence of computer code concerning the Exploit.

f. Evidence concerning Anton and James trading strategies and use of MEV Bots.

g. Evidence of knowledge by Anton and James concerning the purpose of the Exploit, including the ability to lure particular MEV bots to certain transactions and obtain access to private trading data.

h. Evidence of concealment of the Exploit and the funds obtained from the Exploit.

i. Evidence of unlawful agreements, including to commit fraud, misappropriate commodities transactions, gain unauthorized computer access, and/or engage in money laundering.

j. Evidence establishing the relationship amongst Anton, James, and/or any other co-conspirators.

k. Evidence of the receipt, transfer, disposition, or location of funds raised through the commission of the Subject Offenses.

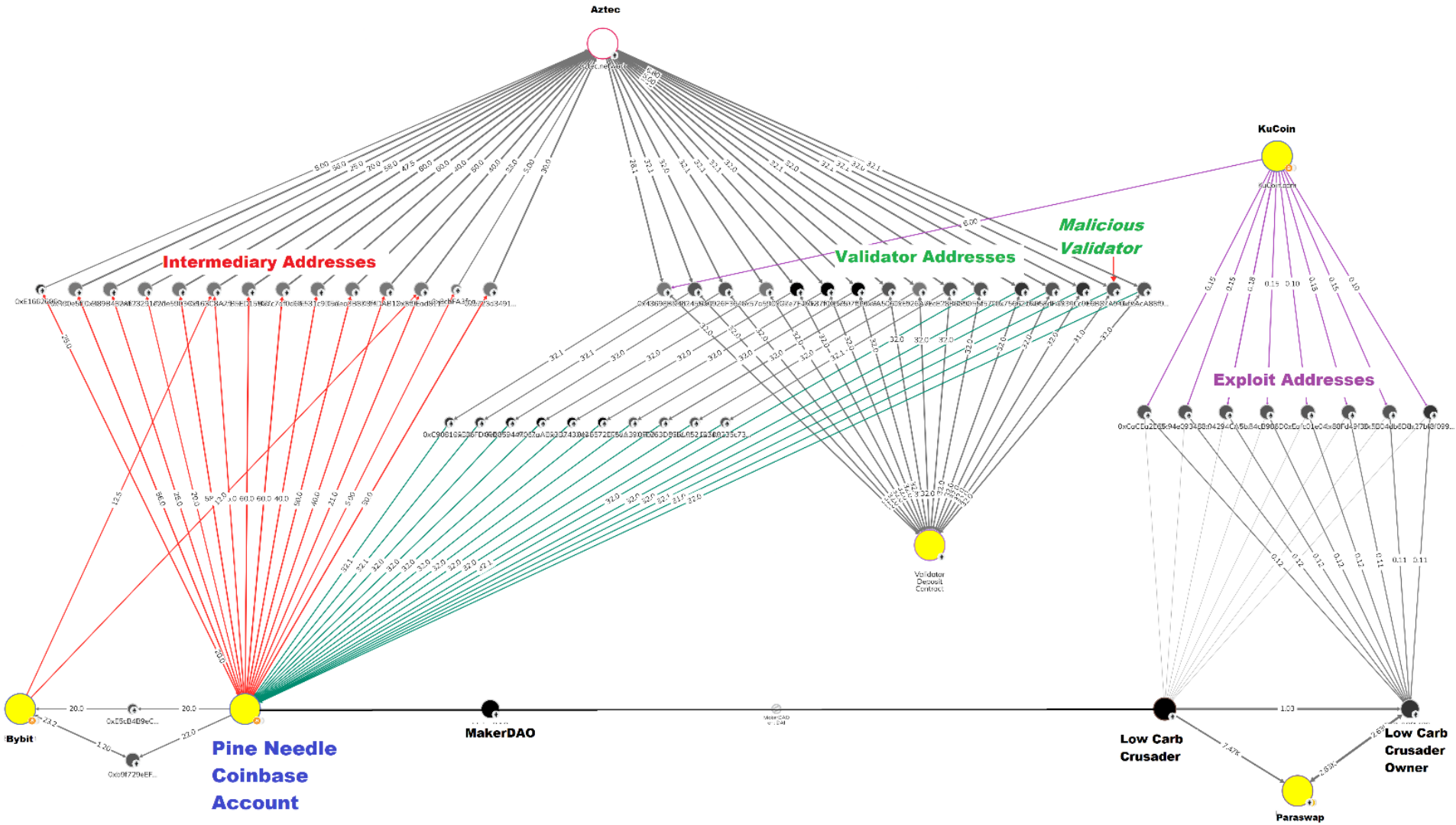
l. Evidence of efforts to conceal the commission of the Subject Offenses and evade detection by law enforcement and/or regulatory agencies.

m. Evidence of the geographic location of the users of the Subject Accounts.

n. Evidence of passwords or other information needed to access the Subject Accounts or other accounts of the users of the Subject Accounts.

o. Evidence relating to other accounts, devices, or physical premises in which evidence of the commission of the Subject Offenses may be found.

Appendix 1


Aztec
KuCoin
Intermediary Addresses
Validator Addresses
Malicious Validator
Exploit Addresses
Validator Deposit Contract
Bybit
Pine Needle Coinbase Account
MakerDAO
Low Carb Crusader
Low Carb Crusader Owner
Paraswap